Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

Thursday, November 17, 2005

Secure and accurate time sources

Broadcasts using sound or radiation, from sources such as radio, bell towers, and astronomical phenomena, must send out the same value to every receiver. A remote beacon such as a pulsar has perfect security: the access structure is any party, and its complement, the attack structure, is the empty set. For human controlled broadcasts, the attack structure consists only of the broadcaster and the access structure is any receiver.

Natural broadcasts are thus immune to the problem (known in computer science as the Byzantine Generals problem) of a transmitter sending different values to different receivers. Indeed, distributed network researchers have gone to great lengths to recreate this simple property on the Internet with logical broadcast protocols. The results are incomplete and very inefficient compared to physical broadcasts.

Nature provides clocks that are oblivious to the malicious intentions of any outside parties and many orders of magnitude more accurate than random delays that face attackers on the Internet. If critical Internet servers were synchronized to natural clocks in a secure and timely fashion, they would be immune to attacks that relied on uncertainties in timing. Here are some comparisons of the stability (error creep) in good natural clocks. Pulsars overtake atomic clocks in accuracy after about 4 months.

Oscillator Stability	1 sec	1 day	1 month
Quartz	10^-12	10^-9	10^-8
Rubidium	10^-11	10^-12	10^-11
Cesium Beam	10^-10	10^-13	10^-13
Hydrogen Maser	10^-13	10^-14	10^-13
Pulsar	10^-11	10^-12	10^-13

Posted by Nick Szabo at 6:11 PM

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

3 comments:

David Mercer said...

My home network's clock (set from the network) is sometimes under attack by my cats. They will occasionally get too rambunctious and flip a switch on a powerbar!

11:15 AM

Iang said...

By pulsar, do you mean the star type in the sky or some form of technology?

1:08 PM

Nick Szabo said...

The kind in the incorruptable heavens. Pulsars retain the valuable security property (as with astronomy-based time checks throughout history but unlike atomic clocks) that many people can observe the same "clock ticks" simultaneously and independently.

10:55 AM

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ► 2007 (47)
- ► 2006 (130)
- ▼ 2005 (44)
  - ► December (16)
  - ▼ November (5)
    - Specific cycles, trust minimization, and the kula ...
    - Secure and accurate time sources
    - Commercial payments at the Muslim zenith
    - Metabolite schedule
    - Augustus' solar timekeeper
  - ► October (23)

Simple theme. Powered by Blogger.